KO

Previously in Math 103a

What does it mean for 2 groups to look the same? Interlude from Ch. 6

Def. Let $G, \overline{G}$ be groups. An isomorphism from G to $\overline{G}$ is a mapping $\varphi: G \to \overline{G}$ which is 1-1 & onto (bijective) and respects group operations!

$$\varphi(\underbrace{a \cdot b}_{\text{operation in } G}) = \underbrace{\varphi(a) \cdot \varphi(b)}_{\text{operation in } \overline{G}}$$

If such a φ exists, then G & $\overline{G}$ are said to be isomorphic, written $\boxed{G \approx \overline{G}}$ or $G \cong \overline{G}$.

Note: $\approx$ is an equivalence relation on set of groups. Some stuff to check!

Many examples.

Ex 1. Let G & $\bar{G}$ be cyclic groups. Then

$$\boxed{G \approx \bar{G} \iff |G| = |\bar{G}|}$$

Check: For $\Rightarrow$ use contrapositive, show that if $|G| \neq |\bar{G}|$, then $G \not\approx \bar{G}$. This is easy, since if $|G| \neq |\bar{G}|$ there is no bijection $\varphi: G \to \bar{G}$.

Check $\Leftarrow$. Suppose first $|G| = |\bar{G}| = n < \infty$

Let $a \in G$ be a generator of G and $\bar{a} \in \bar{G}$ a generator of $\bar{G}$

Then $G = \{e, a, a^2, \dots, a^{n-1}\}$

$\bar{G} = \{e, \bar{a}, \bar{a}^2, \dots, \bar{a}^{n-1}\}$

Define $\varphi: G \to \bar{G}$ by $\varphi(a^k) = \bar{a}^k$, $k = 0, 1, \dots, n-1$

φ is a bijection. Need to check

$$(*)\ \varphi(a^k a^\ell) = \varphi(a^k)\varphi(a^\ell)$$

Let $m = (k+\ell) \bmod n$. Then

$$\varphi(a^k a^\ell) = \varphi(a^{k+\ell}) = \varphi(a^m) = \bar{a}^m = \bar{a}^{k+\ell} = \bar{a}^k \bar{a}^\ell = \varphi(a^k)\varphi(a^\ell)$$

This proves $(*)$!

If $\underline{|G| = |\bar{G}| = \infty}$ and a generates G, $\bar{a}$ generates $\bar{G}$

$G = \{e, a, a^2, \dots, a^n, \dots\}$ $\quad$ $\bar{G} = \{e, \bar{a}, \bar{a}^2, \dots, \bar{a}^n, \dots\}$

put $\boxed{\varphi(a^k) = \bar{a}^k.}$ Then

$\varphi(a^k a^l) = \varphi(a^{k+l}) = \bar{a}^{k+l} = \bar{a}^k \bar{a}^l$, so φ is an isomorphism of G & $\bar{G}$

<u>Ex 2.</u> $G = U(5)$, $\bar{G} = \mathbb{Z}_4$.

$\boxed{U(5) = \{1, 2, 3, 4\}}$ $\quad$ $\boxed{\mathbb{Z}_4 = \{0, 1, 2, 3\}}$

oper. = multiplication mod 5 $\quad$ oper. = addition mod 4

$U(5)$ is generated by 2 & 4 cyklic $\quad$ $\mathbb{Z}_4$ generated by 1 & 3 cyclic.

Isomorphic by Ex 1.

Let's take $a = 2$, $\bar{a} = 1$, $\varphi(a^k) = \bar{a}^k$

group operation in $\bar{G}$

$$\varphi(2) = 1$$
$$\varphi(2^2) = \varphi(4) = \varphi(2) + \varphi(2) = 1 + 1 = 2$$
$$\varphi(2^3) = \varphi(3) = \varphi(2) + \varphi(2) + \varphi(2) = 3$$
$$\varphi(2^4) = \varphi(1) = 4\varphi(2) = 0$$

Isomorphism is
$$\varphi: \begin{array}{l} 2 \longmapsto 1 \\ 4 \longmapsto 2 \\ 3 \longmapsto 3 \\ 1 \longmapsto 0 \end{array}$$

Ex 3. $G = U(8) = \{1, 3, 5, 7\}$ not cyclic

$\bar{G} = \{5, 15, 25, 35\}$ multiplication mod 40

This was a homework problem!

The trick is that $(25)^2 \bmod 40 = 25$, $(**)$

So 25 is the identity in $\bar{G}$. An isomorphism φ must take identity to identity
in G in $\bar{G}$

Put
$$\boxed{\begin{aligned} \varphi(1) &= 25 \in \bar{G} \\ \varphi(3) &= 3 \times 25 \bmod 40 = 35 \\ \varphi(5) &= 5 \times 25 \bmod 40 = 5 \\ \varphi(7) &= 7 \times 25 \bmod 40 = 15 \end{aligned}}$$

Why this works: $\varphi(a \cdot b) = 25\,ab \bmod 40$

$$\begin{aligned} \varphi(a) \cdot \varphi(b) &= (25a)(25b) \bmod 40 \\ &= (25)^2 ab \bmod 40 \\ &= 25\,ab \bmod 40 \end{aligned}$$

by $(**)$

Ex 4

$G = \mathbb{R}$ addition, $\bar{G}$ = positive reals, multiplication

Put $\varphi(a) = 2^a$

Then $\varphi(a+b) = 2^{a+b} = 2^a 2^b$

Bijection? $2^a = 2^b \Leftrightarrow 2^{a-b} = 1 \Leftrightarrow a - b = 0 \Rightarrow$ 1-1

If $y > 0$, then $\log_2 y \in \mathbb{R}$, $2^{\log_2 y} = y \Rightarrow$ onto

Ex 5. If G is a cyclic group of order n, how many different isomorphisms are there from G to G?

Terminology: An isomorphism $G \to \bar{G}$ is called an **automorphism** if $\bar{G} = G$.

Ans. Let a be a generator of G, so that

$G = \{e, a, a^2, \ldots, a^{n-1}\}$

By previous theorem, a^k is a generator of $G \iff \gcd(k, n) = 1$.

$\therefore \exists\ \varphi(n)$ different automorphisms of G.

phi function

Note: If φ is an isomorphism $G \to \bar{G}$ & $\varphi(a) = \bar{a}$, then $|a| = |\bar{a}|$. check it!

Ex 6 $\boxed{U(10) \not\approx U(12)}$

$U(10) = \{1, 3, 7, 9\}$ cyclic, 3 is a generator.

$U(12) = \{1, 5, 7, 11\}$

$5^2 \bmod 12 = 1$

$7^2 \bmod 12 = 1$

$11^2 \bmod 12 = 1$

not cyclic

$|3| = 4$ in $U(10)$

$|\bar{a}| \leq 2 \quad \forall\ \bar{a} \in U(12)$

so no isomorphism.

Ex 7. $\mathbb{R}$ addition, $\mathbb{R}^*$ non zero reals multiplication

$\mathbb{R} \not\cong \mathbb{R}^*$

Reason: If $\varphi: \mathbb{R} \longrightarrow \mathbb{R}^*$ onto

$\exists\, a \in \mathbb{R}$ s.t. $\varphi(a) = -1$.

If φ is an isom, then

$$-1 = \varphi(a) = \varphi\left(\tfrac{1}{2}a + \tfrac{1}{2}a\right) = \left(\varphi\left(\tfrac{1}{2}(a)\right)\right)^2$$

$\varphi\left(\frac{1}{2}(a)\right)$ is a real number, but there is no real number x with $x^2 = -1$

Note: to show 2 groups are isomorphic, need to find just 1 isomorphism.
To show 2 groups are not isomorphic, need to show any bijection is not an isomorphism. This can be tough!

Ex 8. There is no isomorphism from

$\mathbb{Q} \longrightarrow$ positive rationals

addition multiplication

Reason: 2 is a positive rational. If φ is a bijection $\exists!\, a \in \mathbb{Q}$ with $\varphi(a) = 2$.

Then $\varphi\left(\frac{a}{2} + \frac{a}{2}\right) = \left(\varphi\left(\frac{a}{2}\right)\right)^2 = 2$ if φ is isom.

But $\nexists$ r rational with $r^2 = 2$.

K6

Ex 4. Automorphisms of $SL(2,\mathbb{R})$

$$= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \; a,b,c,d \in \mathbb{R}, \ \det = 1 \right\}$$

Let $M \in GL(2,\mathbb{R})$ (invertible 2×2 matrices)

Define $\varphi_M : SL(2,\mathbb{R}) \longrightarrow SL(2,\mathbb{R})$

(also written $SL(2,\mathbb{R}) \circlearrowleft$)

by $\boxed{\phi_M(A) = MAM^{-1}}$ $\forall\, A \in SL(2,\mathbb{R})$

Claim φ_M is an isom

① $\varphi_M(A) \in SL(2,\mathbb{R})$, since $\det(MAM^{-1})$

$$= (\det M)(\det A)(\det M^{-1})$$
$$= (\det M)(\det M)^{-1}$$
$$= 1$$

② φ_M is 1-1; $MAM^{-1} = MBM^{-1} \Longleftrightarrow A = B$ (cancellation)

(3) φ_M is onto: for $B \in SL(2,\mathbb{R})$,

$$\varphi(M^{-1}BM) = M(M^{-1}BM)M^{-1} = B.$$

(4) Preserves products:

$$\boxed{\begin{aligned} \varphi_M(AB) &= MABM^{-1} = MAM^{-1}MBM^{-1} \\ &= \varphi_M(A)\varphi_M(B) \end{aligned}}$$